Claims

[c1] I claim:

A method for intrusion detection of a computer system that identifies prior to execution computer system objects that have been changed or new objects added by unauthorized entities. Said method comprises the phases of definition, creation and authentication.

[c2] The method of claim 1, further comprising the steps of the intrusion detection environment definition.

[c3] The method of claim 2, wherein comprises the step of defining the DNA Domain, which is the environment where computer system objects reside, and is managed by the DNA Domain Administrator, who is an individual or group responsible for authorizing new objects to enter the DNA Domain.

[c4] The method of claim 2, wherein comprises the step of defining the DNA Scope Set, which is a set of objects, coined DNA Objects, residing in the DNA Domain having the same DNA Pattern, which is defined in method 6.

[c5] The method of claim 2, wherein comprises the step of defining an external data storage structure (EDSS) that is a container for control information for the intrusion detection system.

[c6] The method of claim 2, wherein comprises the step of defining the DNA Pattern, which is a sequence of identifier fields that will serve to create a unique copy of the object and create an ownership token between the object and the operating system.

[c7] The method of claim 6, wherein the DNA Pattern is selected from the properties of the computer system objects (DNA Objects) in the DNA Scope Set such that the DAN Pattern is unique across the DNA Domain when compared to other DNA Patterns.

[c8] The method of claim 6, wherein further comprises the step of storing the DNA Pattern in the EDSS.

[c9] The method of claim 1, further comprising the steps of the creation phase, which inserts the DNA Pattern into DNA Scope Set objects creating DNA Steganographic Objects.

[c10] The method of claim 9, wherein comprises the step of selecting DNA Objects from the DNA Domain to be protected.

[c11] The method of claim 9, wherein comprises the step of retrieving the DNA Pattern from the EDSS.

[c12] The method of claim 9, wherein comprises the step of encrypting the DNA Pattern.

[c13] The method of claim 9, wherein comprises the step of a steganographic process to embed the results of method 12 into the results of method 10 producing a DNA Steganographic Object.

[c14] The method of claim 9, wherein comprises the step of storing the results of method 13 in the system resource library.

[c15] The method of claim 14, further comprises the step of moving the original DNA Object off-line.

[c16] The method of claim 9, wherein comprises the step of storing control information into an EDSS file record relative to the DNA Steganographic Object so as to be able to extract the DNA Pattern from the DNA Steganographic Object and recreate the DNA Object.

[c17] The method of claim 1, further comprising the steps of the authentication phase, which extracts a DNA Pattern from the DNA Steganographic Object (the results of method 13) recreating the DNA Object.

[c18] The method of claim 17, wherein comprises the step of the operating system providing the intrusion detection system with an object name to be executed.

[c19] The method of claim 17, wherein comprises the step of searching the EDSS for a record containing a DNA Steganographic Object having the same name as the results of method 18.

[c20] The method of claim 17, wherein the object is rejected is the object name is not found on the EDSS.

[c21] The method of claim 17, wherein comprises the step of extracting control information from a record corresponding to the DNA Steganographic Object of the EDSS file.

[c22] The method of claim 17, wherein comprises the step of, given the control information from method 21, reversing the steganographic process of method 13 to extract the encrypted DNA Pattern.

[c23] The method of claim 22, further comprises the step of recreating the DNA Object.

[c24] The method of claim 22, further comprises the step of decrypting the DNA Pattern.

[c25] The method of claim 17, wherein comprises the step of retrieving the DNA Pattern definition from the EDSS file.

[c26] The method of claim 17, wherein comprises the step of comparing the results of method 24 with the results of method 25.

[c27] The method of claim 26, wherein further authenticates the object for execution if there is a match.

[c28] The method of claim 26, wherein further rejects the object if there is no match.